



DEPARTMENT OF THE AIR FORCE

Headquarters Air Force Materiel Command
Wright-Patterson Air Force Base Ohio

64-10
Part 27
Fountain
29 Oct 99

MEMORANDUM FOR SEE DISTRIBUTION

19 Oct 99

FROM: HQ AFMC/PK
4375 Chidlaw Road, Suite 6
Wright-Patterson AFB OH 45433-5006

SUBJECT: Foreign National Access to Unclassified Air Force Information Systems

1. The attached memorandum implements AFMC's policy on foreign national access to unclassified information systems. This policy will be incorporated as AFMC Supplement 1 to AFI 33-202, Computer Security. Foreign nationals legally admitted as permanent residents or as Green Card holders are not covered by the policy. The policy delineates the responsibilities of the organizations involved in the access approval process and delegates final approval authority to AFMC/CV.
2. While contracting is not directly involved in the access approval process, you should consider the requirement in your acquisition strategy to ensure proper procedures are followed before awarding a contract.
3. If you have any questions, please contact Major Doug Wells, HQ AFMC/PKP at DSN 787-0181, or E-mail at Douglas.Wells@wpafb.af.mil.

/s/

MILTON C. ROSS, SES
Deputy Director of Contracting

Attachment:
AFMC/CC Memo, 28 Sep 99, w/Atch

2000-2-M

DISTRIBUTION:

AAC/PK
AEDC/PK
AFFTC/PK
AFRL/PK
ASC/PK
ESC/PK
311th HSW/PK
OC-ALC/PK
OO-ALC/PK
SA-ALC/PK
SM-ALC/PK
SMC/PK
WR-ALC/PK

CC:

AFOSR/PK
AFRL/HEK
AFRL/IFK
AFRL/MNK
DET 1 AFRL/PK
DET 8 AFRL/PK
38 LS/LGC
CPSG/RMK
ESC/PIW
OO-ALC/PKL
MSG/PK
SSG/PK

HQ AFMC/PKA/PKL/PKO/PKP/PKS/PKT/PKX



DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR FORCE MATERIEL COMMAND
WRIGHT-PATTERSON AIR FORCE BASE, OHIO

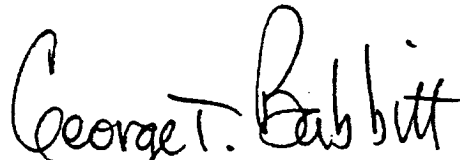
SEP 28 1999

MEMORANDUM FOR ALAFMC (COMMANDER/DIRECTOR/CHIEF)

FROM: AFMC/CC
4375 Chidlaw Road, Suite 1
Wright-Patterson AFB OH 45433-5001

SUBJECT: Foreign National Access to Unclassified Air Force Information Systems

1. This memorandum directs implementation of AFMC policy on Foreign National Access to AFMC Unclassified Information Systems (see attached), IAW with AFI 33-202. The policy will be incorporated in the issuance of AFI 33-202, AFMC Supplement 1.
2. Further, AFI 33-202 states that the MAJCOM commanders are responsible for authorizing foreign national access to unclassified information systems within their respective commands, and authority may not be delegated below the MAJCOM vice commander. Accordingly, I have delegated responsibility for authorizing foreign national access to unclassified AFMC information systems to AFMC/CV. Requests for access to the Defense Information System Network must be validated by AFMC/CV, validated by Joint Staff/J6 and approved by the Office of the Secretary of Defense.
3. Compliance with the attached policy is mandatory. Our point of contact is Mrs. Debra Haley, Director, Communications and Information, HQ AFMC/SC, DSN 787-3626, commercial (937) 257-3626, or e-mail: debra.haley@wpafb.af.mil. The functional point of contact is Fred Pacifico, AFMC CSO/SCSN, DSN 986-0920, commercial (937) 656-0920, or email: fred.pacifico@wpafb.af.mil.


GEORGE T. BABBITT
General, USAF
Commander

Attachment:
Policy on Foreign National Access

cc:
AFMC/CV w/o Atch

**POLICY
ON
FOREIGN NATIONAL ACCESS TO THE
AIR FORCE UNCLASSIFIED INFORMATION SYSTEMS**

In accordance with AFI 33-202, Computer Security, 1 Feb 99, the following outlines AFMC policy and procedures on granting foreign national access to unclassified Air Force information systems. AFI 33-202 provides direction for access to the Air Force systems not DoD systems; therefore, access to the High Performance Computing (HPC) Modernization Program (HPCMP) resources do not fall under the purview of Air Force policy. However, we must implement current Air Force policy for access to Air Force systems and access to systems (i.e., HPC systems) via the AFMC backbone.

1. References:

- a. DoDD 5200.28, Security Requirements for Automated Information Systems (AISs), 21 Mar 88
- b. DoD 5200.2-R, Personnel Security Program, Jan 87
- c. DoDD 5230.20, Visits, Assignments, and Exchanges of Foreign Nationals, 12 Aug 98
- d. AFI 31-501, Personnel Security Program Management, May 94

2. Definition:

Foreign National: Any person who is not a citizen or national of the United States. This **does not include** foreign nationals who are legally admitted to the United States as permanent residents.

3. Responsibilities:

- 3.1 **The requesting organization** will prepare a request package to include the following:
 - 3.1.1 Staff summary sheet (SSS) with coordination blocks for the servicing Foreign Disclosure Office, the servicing Information Security Program Manager, the local Designated Approval Authority (DAA), the Unit Security Manager, and the local Information Assurance Office. The local Information Assurance Office should be the last one to coordinate on the package.
 - 3.1.2 Request memorandum with justification detailing the requirement for access, type of information to be accessed and duration of access, and category of the position the subject will occupy IAW DoD 5200.2-R (Tab 1).
 - 3.1.3 As applicable: A verification of a current Personnel Security Investigation (PSI), Single Scope Background Investigation, National Agency Check of the appropriate level, or Security Assurance from the subject's country (Tab 2).
 - 3.1.4 The information required IAW with AFI 33-202, Section 3.7 (Tab 3).
- 3.2 **The Servicing Foreign Disclosure Office** will determine if the types/categories of information requested is releasable, prepare a memorandum explaining any specific requirements (Tab 4), and coordinate on the SSS concurring or nonconcurring with the request. Access by foreign exchange officers who are filling a USAF billet and thus performing the duties of a USAF officer should be limited to the established terms and agreements between DoD and the exchange officer's parent country.

- 3.3 The Servicing Information Security Program Manager will verify that the subject has a current PSI, and coordinate on the SSS to indicate the required actions have been completed.
- 3.4 The Local DAA will coordinate on the SSS endorsing or not endorsing it and prepare a memorandum to ensure the following (Tab 5):
- 3.4.1 The system is certified and accredited and attach the System Security Authorization Agreement and/or the Certification and Accreditation information.
 - 3.4.2 The Computer System Manager and the Computer System Security Officer have the computer security in place to assure that only authorized information is accessible, as defined by the Foreign Disclosure Office.
 - 3.4.3 IAW AFSSI 5024, include the risk and vulnerability assessment which must address the potential vulnerability of access by foreign nationals. The system/network must have safeguards present to ensure that the foreign national only has permission to access only the types/categories of information determined to be releasable by the servicing foreign disclosure office. This is to include restricting the individual from .mil/gov web sites, as appropriate. It may require providing the individual a stand-alone computer with a dial-in capability to a commercial internet service provider.
- 3.5 The Local Information Assurance Office will review the package to ensure completeness, coordinate on the SSS concurring or nonconcurring on the request, maintain the official file of the package, and submit the package to the HQ AFMC Information Assurance Office (AFMC CSO/SCSN).
- 3.6 The HO AFMC Information Assurance Office will review the package to ensure completeness, prepare a staff summary for validation/approval through OSD as necessary, obtain coordination from HQ staff as appropriate, and forward the request to AFMC/CV.
- 3.7 AFMC/CV will:
- 3.7.1 Approve/disapprove foreign national access to unclassified information systems/networks within AFMC, and send approved/disapproved package to the HQ AFMC Information Assurance Office (AFMC CSO/SCSN) to be forwarded to the local Information Assurance Office.
 - 3.7.2 Validate and submit requests for access to Air Force systems and the Defense Information System Network to AF/SC for Joint Staff/J6 validation and approval through the Office of the Secretary of Defense. AF/SC will send the approved/disapproved package to the HQ AFMC Information Assurance Office (AFMC CSO/SCSN) to be forwarded to the local Information Assurance Office."

Process on Foreign National Access to Air Force Unclassified Information Systems

